Optimal Entanglement Witnesses for Qubits and Qutrits

Reinhold A. Bertlmann, Katharina Durstberger, Beatrix C. Hiesmayr, and Philipp Krammer

Institute for Theoretical Physics, University of Vienna,
Boltzmanngasse 5, A-1090 Vienna, Austria

We study the connection between the Hilbert-Schmidt measure of entanglement (that is the minimal distance of an entangled state to the set of separable states) and entanglement witness in terms of a generalized Bell inequality which distinguishes between entangled and separable states. A method for checking the nearest separable state to a given entangled one is presented. We illustrate the general results by considering isotropic states, in particular 2-qubit and 2-qutrit states – and their generalizations to arbitrary dimensions – where we calculate the optimal entanglement witnesses explicitly.

I. INTRODUCTION

Quantum entanglement is one of the most remarkable features of quantum mechanics [1, 2]. In the last years it became clear that it can serve as a source for various tasks in quantum information theory (see, e.g., Ref. [3]). Much attention has been paid to explore the possibilities of applying quantum systems to communication and computing protocols. Usually, these protocols use the information encoded in qubit systems; however, higher dimensional systems, e.g. qutrits, are of increasing interest (see, e.g., [4]). Therefore it is important to get a more accurate description of entanglement, especially for higher dimensional systems, which includes detecting and measuring entanglement (for an overview see, e.g., Refs. [5, 6]). For pure states such a description is rather simple whereas for mixed states it is is more complicated.

The detection of entanglement, that is, distinguishing between separable and entangled states, has become easy for 2-qubit states only. In this case necessary and sufficient conditions for separability have been found [7, 8], whereas for higher dimensions there exist in general only necessary conditions for separability. In general, one can define several types of entanglement measures, for instance, entanglement of formation [9], the concurrence [10, 11] or the so called distance measures [12, 13].

In this paper a particular distance measure is used, the Hilbert-Schmidt distance, which quantifies the distance of an entangled state to the set of all separable states. It is discussed as an entanglement measure in Refs. [14, 15]. We will call this measure shortly Hilbert-Schmidt measure. In Ref. [16] it is shown that the Hilbert-Schmidt measure of an entangled state equals the maximal violation of the generalized Bell inequality which will be discussed in this article.

The paper is organized as follows: In Sect. II we discuss the mathematical basic concepts and definitions. In Sect. III we re-examine shortly the results of Ref. [16] in order to get a lemma for determining the nearest separable state to an entangled state. In Sect. IV and

Sect. V we then illustrate our general results for the cases of isotropic qubit and qutrit states. Finally, in Sect. VI we discuss isotropic states in arbitrary dimensions.

II. CONCEPTS AND DEFINITIONS

A. Bipartite Systems in a Finite Dimensional Hilbert Space

In this article we consider bipartite systems in a $d \times d$ dimensional Hilbert space $\mathcal{H}_A^d \otimes \mathcal{H}_B^d$. The observables acting in the subsystems $\mathcal{H}_A$ and $\mathcal{H}_B$ are usually called Alice and Bob in quantum communication. Observables are represented by Hermitian matrices and states by density matrices.

A state ρ is called *separable* if it can be written as a convex combination of product states:

$$\rho_{\text{sep}} = \sum_i p_i \, \rho_A^i \otimes \rho_B^i, \qquad 0 \le p_i \le 1, \; \sum_i p_i = 1 \,. \tag{1}$$

All states satisfying Eq. (1) form the set of separable states S. If a state is not separable, i.e., it cannot be written in terms of Eq. (1), then it is called *entangled*.

We define an *isotropic* state ρ_α by (see Refs. [6, 17, 18])

$$\rho_\alpha = \alpha \left| \phi_+^d \right\rangle \left\langle \phi_+^d \right| + \frac{1-\alpha}{d^2} \mathbb{1} \,, \quad \alpha \in \mathbb{R} \,, \quad -\frac{1}{d^2-1} \le \alpha \le 1 \,, \tag{2}$$

where the range of α is determined by the positivity of the state. The state $\left| \phi_+^d \right\rangle$ is maximally entangled and given by

$$\left| \phi_+^d \right\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle_A \otimes |i\rangle_B \,, \tag{3}$$

where $\{|i\rangle\}$ is an orthonormal basis in $\mathcal{H}^d$.

The state is called isotropic because it is invariant under any $U_A \otimes U_B^*$ transformations (see Ref. [17])

$$(U_A \otimes U_B^*) \rho_\alpha (U_A \otimes U_B^*)^\dagger = \rho_\alpha \,, \tag{4}$$

where U is a unitary operator, U^* is its complex conjugate. The isotropic state ρ_α has the following properties:

$$\begin{aligned} -\frac{1}{d^2-1} \le \alpha \le \frac{1}{d+1} &\quad \Rightarrow \quad \rho_\alpha \text{ separable} \,, \\ \frac{1}{d+1} < \alpha \le 1 &\quad \Rightarrow \quad \rho_\alpha \text{ entangled} \,. \end{aligned} \tag{5}$$

Operators on a finite dimensional Hilbert space are elements of another Hilbert space themselves, called Hilbert-Schmidt space $\mathcal{A} = \mathcal{A}_A \otimes \mathcal{A}_B$. In this space the scalar product between two elements is defined as

$$\langle A, B \rangle = \text{Tr} \, A^\dagger B \qquad A, B \in \mathcal{A} \,, \tag{6}$$

with the corresponding Hilbert-Schmidt norm

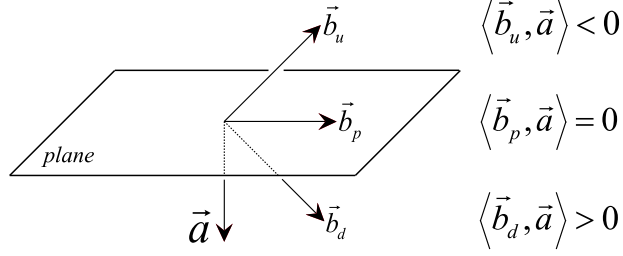$$\|A\| = \sqrt{\langle A, A \rangle} \qquad A \in \mathcal{A} \,. \tag{7}$$

FIG. 1: Geometric illustration of a plane in Euclidean space and the different values of the scalar product for states above ($\vec{b}_u$), within ($\vec{b}_p$) and below ($\vec{b}_d$) the plane.

Example for qubits. In case of Alice and Bob acting on a Hilbert space $\mathcal{H}_A^2 \otimes \mathcal{H}_B^2$, an arbitrary observable A can be written in the form

$$A = a\, \mathbb{1}_A \otimes \mathbb{1}_B + a_i\, \sigma_A^i \otimes \mathbb{1}_B + b_i\, \mathbb{1}_A \otimes \sigma_B^i + c_{ij}\, \sigma_A^i \otimes \sigma_B^j, \quad a, a_i, b_i, c_{ij} \in \mathbb{R}\,. \qquad (8)$$

Note that c_{ij} can be diagonalized by 2 independent orthogonal transformations on σ_A^i and σ_B^j [19]. The operator A represents a density matrix if $a = 1/4$ and $\sum_i (a_i^2 + b_i^2) + \sum_{i,j} c_{ij}^2 \leq 1/16$.

With help of the norm (7) we can quantify a distance between two arbitrary states ρ_1, ρ_2, the *Hilbert-Schmidt distance*,

$$d_{\mathrm{HS}}(\rho_1, \rho_2) = \|\rho_1 - \rho_2\|\,. \qquad (9)$$

Viewing the Hilbert-Schmidt distance as an entanglement measure (see Refs. [14, 15]) we define the so-called *Hilbert-Schmidt measure*

$$D(\rho_{\mathrm{ent}}) = \min_{\rho \in S} d_{\mathrm{HS}}(\rho, \rho_{\mathrm{ent}}) = \min_{\rho \in S} \|\rho - \rho_{\mathrm{ent}}\|\,, \qquad (10)$$

which is the minimal distance of an entangled state ρ_{ent} to the set of separable states.

An *entanglement witness* $A \in \mathcal{A}$ is a Hermitian operator that 'detects' the entanglement of a state ρ_{ent} via inequalities [8, 16, 20, 21]

$$\begin{aligned}
\langle \rho_{\mathrm{ent}}, A \rangle = \mathrm{Tr}\, \rho_{\mathrm{ent}} A &< 0\,, \\
\langle \rho, A \rangle = \mathrm{Tr}\, \rho A &\geq 0 \qquad \forall \rho \in S\,.
\end{aligned} \qquad (11)$$

Geometric illustration. For a geometrical illustration of the above inequalities let us consider the following: In Euclidean space a plane is defined by its orthogonal vector $\vec{a}$. The plane separates vectors which have a negative scalar product with $\vec{a}$ from vectors having a positive one; vectors in the plane have, of course, a vanishing scalar product (see Fig. 1).

This can be compared with our situation: A scalar functional $\langle \rho, A \rangle = 0$ defines a hyperplane in the set of all states, and this plane separates 'left-hand' states ρ_l satisfying $\langle \rho_l, A \rangle < 0$ from 'right-hand' states ρ_r with $\langle \rho_r, A \rangle > 0$. States ρ_p with $\langle \rho_p, A \rangle = 0$ are inside the hyperplane. According to the Hahn-Banach theorem, one can conclude that due to the convexity of the set of separable states, there always exists a plane that separates an entangled state from the set of separable states.
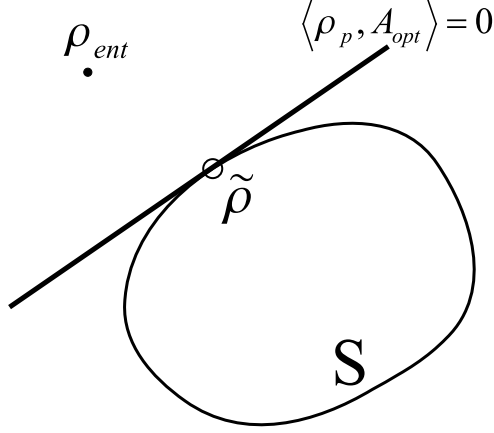
FIG. 2: Illustration of an optimal entanglement witness

An entanglement witness is 'optimal', denoted by A_{opt}, if apart from Eq. (11) there exists a separable state $\tilde{\rho} \in S$ such that

$$\langle \tilde{\rho}, A_{opt} \rangle = 0 \,. \tag{12}$$

It is optimal in the sense that it defines a tangent plane to the set of separable states S and is therefore called *tangent functional* [16]; see Fig. 2.

According to Ref. [16], we call the lower one of the inequalities (11) a *generalized Bell inequality*, short GBI. 'Generalized' means that it detects entanglement and not just non-locality. Thus it doesn't serve as a criterion to distinguish between a local hidden variable (LHV) theory and quantum theory as the usual Bell inequality does. However, pay attention that in literature the term 'generalized Bell inequalities' is also often used for inequalities that detect non-locality, but are of more general form (more measurements, etc.) than Bell's original inequality (see, e.g., Refs. [20, 22]). Bell inequalities, like the CHSH inequality (Clauser, Horne, Shimony, Holt) [23]

$$\langle \rho, 2\mathbb{1} - B \rangle \geq 0 \,, \qquad B = \vec{a} \cdot \vec{\sigma} \otimes (\vec{b} + \vec{b}') \cdot \vec{\sigma} + \vec{a}' \cdot \vec{\sigma} \otimes (\vec{b} - \vec{b}') \cdot \vec{\sigma} \,, \tag{13}$$

with unit vectors $\vec{a}, \vec{a}', \vec{b}, \vec{b}' \in \mathbb{R}^3$ do *not* necessarily detect entanglement. But the inequality (13) has to be satisfied by any state ρ that admits a LHV model. There exist examples of entangled states – so-called Werner states [24] – that do not violate the CHSH inequality. Nevertheless, *every* entangled state violates the GBI for an appropriate entanglement witness A.

Let us re-write Eq. (11) as

$$\langle \rho, A \rangle - \langle \rho_{\text{ent}}, A \rangle \geq 0 \qquad \forall \rho \in S \,. \tag{14}$$

The *maximal* violation of the GBI is defined by

$$B(\rho_{\text{ent}}) = \max_{A, \|A - a\mathbb{1}\| \leq 1} \left(\min_{\rho \in S} \langle \rho, A \rangle - \langle \rho_{\text{ent}}, A \rangle \right) , \tag{15}$$

where the maximum is taken over all possible entanglement witnesses A, suitably normalized, and a is the coefficient of the unity term of the general expression (8). A general expression for quantifying entanglement with entanglement witnesses can be found in Ref. [25].

B. Qubits

A qubit state ω, acting on $\mathcal{H}^2$, can be decomposed into Pauli matrices

$$\omega \;=\; \frac{1}{2}\left(\mathbb{1} + n_i\,\sigma^i\right), \qquad n_i \in \mathbb{R}\,, \quad \sum_i n_i^2 = |\vec{n}|^2 \leq 1\,. \tag{16}$$

Note that for $|\vec{n}|^2 < 1$ the state is mixed (corresponding to $\mathrm{Tr}\,\omega^2 < 1$) whereas for $|\vec{n}|^2 = 1$ the state is pure ($\mathrm{Tr}\,\omega^2 = 1$).

We can write any density matrix of 2-qubits ρ acting on $\mathcal{H}^2 \otimes \mathcal{H}^2$ (for convenience we drop the indices A and B from now on) in a basis of 4×4 matrices, the tensor products of the identity matrix $\mathbb{1}$ and the Pauli matrices σ^i,

$$\rho \;=\; \frac{1}{4}\left(\mathbb{1} \otimes \mathbb{1} \;+\; a_i\,\sigma^i \otimes \mathbb{1} \;+\; b_i\,\mathbb{1} \otimes \sigma^i \;+\; c_{ij}\,\sigma^i \otimes \sigma^j\right)\,, \qquad a_i, b_i, c_{ij} \in \mathbb{R}\,. \tag{17}$$

A product state $\omega \otimes \rho$ has the form

$$\omega \otimes \rho \;=\; \frac{1}{4}\left(\mathbb{1} \otimes \mathbb{1} \;+\; n_i\,\sigma^i \otimes \mathbb{1} \;+\; m_i\,\mathbb{1} \otimes \sigma^i \;+\; n_i m_j\,\sigma^i \otimes \sigma^j\right)\,,$$
$$n_i, m_i \in \mathbb{R}\,, \quad |\vec{n}| \leq 1\,, \quad |\vec{m}| \leq 1\,. \tag{18}$$

Any separable state can be written as the convex combination of expression (18),

$$\rho_{\mathrm{sep}} \;=\; \sum_k p_k\,\frac{1}{4}\left(\mathbb{1} \otimes \mathbb{1} \;+\; n_i^k\,\sigma^i \otimes \mathbb{1} \;+\; m_i^k\,\mathbb{1} \otimes \sigma^i \;+\; n_i^k m_j^k\,\sigma^i \otimes \sigma^j\right)\,,$$
$$n_i^k, m_i^k \in \mathbb{R}\,, \quad \left|\vec{n}^k\right| \leq 1\,, \quad \left|\vec{m}^k\right| \leq 1\,. \tag{19}$$

C. Qutrits

The description of qutrits is very similar to the one for qubits. A qutrit state ω on $\mathcal{H}^3$ can be expressed in the matrix basis $\{\mathbb{1}, \lambda^1, \lambda^2, \ldots, \lambda^8\}$ with an appropriate set $\{n_i\}$

$$\omega \;=\; \frac{1}{3}\left(\mathbb{1} + \sqrt{3}\,n_i\,\lambda^i\right), \qquad n_i \in \mathbb{R}\,, \quad \sum_i n_i^2 = |\vec{n}|^2 \leq 1\,. \tag{20}$$

The factor $\sqrt{3}$ is included for a proper normalization (see, e.g., Refs. [26, 27]). The matrices λ^i ($i = 1, ..., 8$) are the eight Gell-Mann matrices

$$\lambda^1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \lambda^2 = \begin{pmatrix} 0 & -i & 0 \\ i & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \lambda^3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

$$\lambda^4 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad \lambda^5 = \begin{pmatrix} 0 & 0 & -i \\ 0 & 0 & 0 \\ i & 0 & 0 \end{pmatrix}, \quad \lambda^6 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$

$$\lambda^7 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -i \\ 0 & i & 0 \end{pmatrix}, \quad \lambda^8 = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -2 \end{pmatrix}, \tag{21}$$

with properties $\operatorname{Tr} \lambda^i = 0$, $\operatorname{Tr} \lambda^i \lambda^j = 2\,\delta^{ij}$.

A 2-qutrit state, acting on $\mathcal{H}^3 \otimes \mathcal{H}^3$, can be represented in a basis of 9×9 matrices consisting of the unit matrix $\mathbb{1}$ and the eight Gell-Mann matrices λ^i

$$\rho = \frac{1}{9}\left(\mathbb{1} \otimes \mathbb{1} + a_i\,\lambda^i \otimes \mathbb{1} + b_i\,\mathbb{1} \otimes \lambda^i + c_{ij}\,\lambda^i \otimes \lambda^j\right), \qquad a_i, b_i, c_{ij} \in \mathbb{R}. \qquad (22)$$

By the same argumentation as for qubits any separable 2-qutrit state is a convex combination of product states

$$\rho_{\mathrm{sep}} = \sum_k p_k\,\frac{1}{9}\left(\mathbb{1} \otimes \mathbb{1} + \sqrt{3}\,n_i^k\,\lambda^i \otimes \mathbb{1} + \sqrt{3}\,m_i^k\,\mathbb{1} \otimes \lambda^i + 3\,n_i^k m_j^k\,\lambda^i \otimes \lambda^j\right). \qquad (23)$$

III. CONNECTION BETWEEN HILBERT-SCHMIDT MEASURE AND ENTANGLEMENT WITNESS

A. Geometrical Considerations about the Hilbert-Schmidt Distance

Before we are going to discuss the Bertlmann-Narnhofer-Thirring Theorem [16] let us consider the Hilbert-Schmidt distance. The geometrical illustration we are going to derive turns out to be helpful for the proof of the Theorem.

We can write the Hilbert-Schmidt distance of any two states $\rho_1, \rho_2 \in \mathcal{A}$ as

$$d_{\mathrm{HS}}(\rho_1, \rho_2) = \|\rho_1 - \rho_2\| = \left\langle \rho_1 - \rho_2, \frac{\rho_1 - \rho_2}{\|\rho_1 - \rho_2\|}\right\rangle = \left\langle \rho_1 - \rho_2, \bar{C}\right\rangle. \qquad (24)$$

where we define the operator

$$\bar{C} := \frac{\rho_1 - \rho_2}{\|\rho_1 - \rho_2\|}. \qquad (25)$$

Instead of $\bar{C}$ we may also choose $C := \bar{C} + c\,\mathbb{1}$ $(c \in \mathbb{C})$ and find

$$d_{\mathrm{HS}}(\rho_1, \rho_2) = \left\langle \rho_1 - \rho_2, \bar{C}\right\rangle = \left\langle \rho_1 - \rho_2, \bar{C}\right\rangle + \left\langle \rho_1 - \rho_2, c\,\mathbb{1}\right\rangle = \left\langle \rho_1 - \rho_2, C\right\rangle, \qquad (26)$$

since $\left\langle \rho_1 - \rho_2, \mathbb{1}\right\rangle = \operatorname{Tr}\rho_1 - \operatorname{Tr}\rho_2 = 0$. For convenience we fix c to

$$c = -\frac{\left\langle \rho_1, \rho_1 - \rho_2\right\rangle}{\|\rho_1 - \rho_2\|}, \qquad (27)$$

and obtain

$$C = \frac{\rho_1 - \rho_2 - \left\langle \rho_1, \rho_1 - \rho_2\right\rangle \mathbb{1}}{\|\rho_1 - \rho_2\|}. \qquad (28)$$

Analogously to Euclidean space we define a hyperplane P that includes ρ_1 and is orthogonal to $\rho_1 - \rho_2$ as the set of all states ρ_p satisfying

$$\frac{1}{\|\rho_1 - \rho_2\|}\left\langle \rho_p - \rho_1, \rho_1 - \rho_2\right\rangle = 0. \qquad (29)$$

For all states on one side of the plane, let us call them 'left-hand' states ρ_l, we have
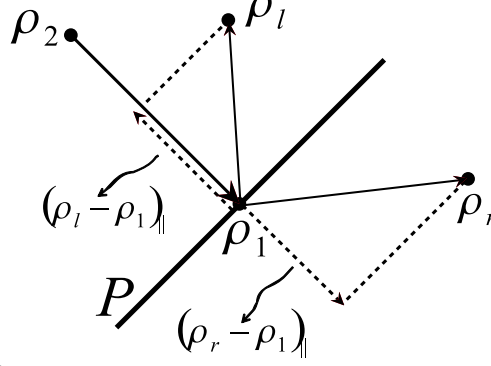
FIG. 3: Illustration of Eqs. (30) and (31): The scalar product $\langle \rho_l - \rho_1, \rho_1 - \rho_2 \rangle$ is *negative* because the projection $(\rho_l - \rho_1)_{\parallel}$ onto $\rho_1 - \rho_2$ points in the opposite direction to $\rho_1 - \rho_2$. On the other side, $\langle \rho_r - \rho_1, \rho_1 - \rho_2 \rangle$ is *positive* for states ρ_r, because then the projection $(\rho_r - \rho_1)_{\parallel}$ points in the same direction as $\rho_1 - \rho_2$.

$$\frac{1}{\|\rho_1 - \rho_2\|} \langle \rho_l - \rho_1, \rho_1 - \rho_2 \rangle \; < \; 0 \,, \tag{30}$$

whereas the states on the other side, the 'right-hand' states ρ_r are given by

$$\frac{1}{\|\rho_1 - \rho_2\|} \langle \rho_r - \rho_1, \rho_1 - \rho_2 \rangle \; > \; 0 \,. \tag{31}$$

For an illustration see Fig. 3.

We can re-write Eqs. (29), (30), and (31) with help of operator C by using

$$\begin{aligned}
\langle \rho \,, C \rangle \; &= \; \left\langle \rho \,, \frac{\rho_1 - \rho_2}{\|\rho_1 - \rho_2\|} \right\rangle - \frac{\langle \rho_1, \rho_1 - \rho_2 \rangle}{\|\rho_1 - \rho_2\|} \, \langle \rho \,, \mathbb{1} \rangle \\
&= \; \frac{1}{\|\rho_1 - \rho_2\|} \langle \rho - \rho_1, \rho_1 - \rho_2 \rangle \,.
\end{aligned} \tag{32}$$

Then the plane P is determined by

$$\langle \rho_p \,, C \rangle \; = \; 0 \,, \tag{33}$$

and the 'left-hand' and 'right-hand' states satisfy the inequalities

$$\langle \rho_l \,, C \rangle \; < \; 0 \quad \text{and} \quad \langle \rho_r \,, C \rangle \; > \; 0 \,. \tag{34}$$

B.   The Bertlmann-Narnhofer-Thirring Theorem

Interestingly, one can find connections between the Hilbert-Schmidt measure and the concept of entanglement witnesses. In particular, there exists the following equivalence stated in the Bertlmann-Narnhofer-Thirring Theorem [16]:

Theorem. The Hilbert-Schmidt measure of an entangled state equals the maximal violation of the GBI:

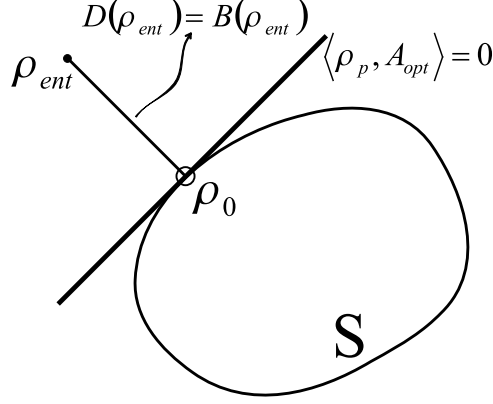$$D(\rho_{\text{ent}}) \; = \; B(\rho_{\text{ent}}) \,. \tag{35}$$

FIG. 4: Illustration of the Bertlmann-Narnhofer-Thirring Theorem

Proof. We want to prove the Theorem in a different way as in Ref. [16].

For an entangled state ρ_{ent} the minimum of the Hilbert-Schmidt distance – the Hilbert-Schmidt measure – is attained for some state ρ_0 since the norm is continuous and the set S is compact

$$\min_{\rho \in S} \|\rho - \rho_{\mathrm{ent}}\| \;=\; \|\rho_0 - \rho_{\mathrm{ent}}\| \;. \tag{36}$$

In Eqs. (26) and (28) we identify $\rho_1 = \rho_0$ and $\rho_2 = \rho_{\mathrm{ent}}$ and with C given by Eq. (28) we obtain the Hilbert-Schmidt measure

$$d_{\mathrm{HS}}(\rho_0, \rho_{\mathrm{ent}}) \;=\; D(\rho_{\mathrm{ent}}) \;=\; \langle \rho_0, C \rangle - \langle \rho_{\mathrm{ent}}, C \rangle \;. \tag{37}$$

In Eq. (37) the operator C has to be an optimal entanglement witness for the following reason: The state ρ_0 lies on the boundary of the set of all separable states S and the hyperplane defined by $\langle \rho_p , C \rangle = 0$ is orthogonal to $\rho_0 - \rho_{\mathrm{ent}}$. Because ρ_0 is the nearest separable state to ρ_{ent} the plane has to be tangent to the set S (see Fig. 4). Eqs. (33), (34) imply the inequalities (11), it therefore follows that C is an optimal entanglement witness

$$A_{opt} \;=\; C \;=\; \frac{\rho_0 - \rho_{\mathrm{ent}} - \langle \rho_0, \rho_0 - \rho_{\mathrm{ent}} \rangle \, \mathbb{1}}{\|\rho_0 - \rho_{\mathrm{ent}}\|} \;, \tag{38}$$

which we use to rewrite the Hilbert-Schmidt measure (37)

$$D(\rho_{\mathrm{ent}}) \;=\; \langle \rho_0, A_{opt} \rangle - \langle \rho_{\mathrm{ent}}, A_{opt} \rangle \;. \tag{39}$$

Note that in general the operator C of Eq. (28) (where ρ_1 and ρ_2 are arbitrary states) is not yet an entanglement witness.

Since the entanglement witness is optimal, i.e.,

$$\max_A \left(- \langle \rho_{\mathrm{ent}}, A \rangle \right) \;=\; - \langle \rho_{\mathrm{ent}}, A_{opt} \rangle \;, \tag{40}$$

where A is restricted by $\|A - a\mathbb{1}\| \leq 1$ and $\langle \rho_0, A_{opt} \rangle = 0$, we obtain

$$D(\rho_{\mathrm{ent}}) \;=\; \langle \rho_0, A_{opt} \rangle - \langle \rho_{\mathrm{ent}}, A_{opt} \rangle \;=\; \max_{A, \|A - a\mathbb{1}\| \leq 1} \left(\langle \rho_0, A \rangle - \langle \rho_{\mathrm{ent}}, A \rangle \right)$$

$$=\; \max_{A, \|A - a\mathbb{1}\| \leq 1} \left(\min_{\rho \in S} \langle \rho, A \rangle - \langle \rho_{\mathrm{ent}}, A \rangle \right) \;=\; B(\rho_{\mathrm{ent}}) \;, \tag{41}$$

which completes the proof.

Similar methods for constructing an entanglement witness can be found in Ref. [28]; for other approaches see, e.g., Refs. [29, 30, 31].
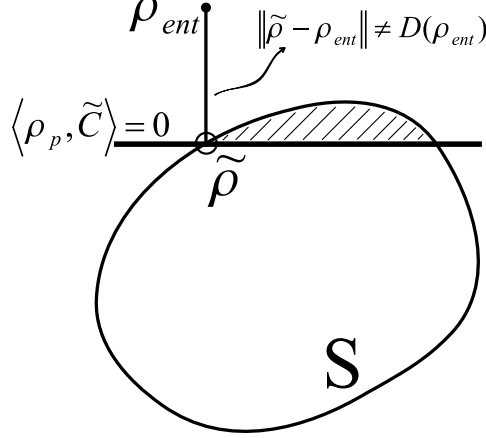
FIG. 5: Illustration why $\tilde{C}$ cannot be an entanglement witness if $\tilde{\rho}$ is not the nearest separable state. The hatched area is the one were the condition $\langle \rho, \tilde{C} \rangle \geq 0 \ \forall \rho \in S$ is violated.

C. How to Check a Guess of the Nearest Separable State

Given an entangled state ρ_{ent}, for the Hilbert-Schmidt measure we have to calculate the minimal distance to the set of separable states S, Eq. (10). In general it is not easy to find the correct state ρ_0 which minimizes the distance (for specific procedures, see, e.g., Refs. [32, 33, 34]). However, we can use an operator like in Eq. (28) for checking a good guess for ρ_0.

How does it work? Let us start with an entangled state ρ_{ent} and let us call $\tilde{\rho}$ the guess for the nearest separable state. From previous considerations (Eqs. (28), (29) and (33)) we know that the operator

$$\tilde{C} \;=\; \frac{\tilde{\rho} - \rho_{\text{ent}} - \langle \tilde{\rho}, \tilde{\rho} - \rho_{\text{ent}} \rangle \, \mathbb{1}}{\|\tilde{\rho} - \rho_{\text{ent}}\|} \tag{42}$$

defines a hyperplane which is orthogonal to $\tilde{\rho} - \rho_{\text{ent}}$ and includes $\tilde{\rho}$. Now we state the following lemma:

> **Lemma.** A state $\tilde{\rho}$ is equal to the nearest separable state ρ_0 if and only if $\tilde{C}$ is an entanglement witness.

Proof. We already know from Sect. III B that if $\tilde{\rho}$ is the nearest separable state then the operator $\tilde{C}$ is an entanglement witness. So we need to prove the opposite: If $\tilde{C}$ is an entanglement witness the state $\tilde{\rho}$ has to be the nearest separable state ρ_0. We prove it indirectly. If $\tilde{\rho}$ is not the nearest separable state then $\|\rho_{\text{ent}} - \tilde{\rho}\|$ does not give the minimal distance to S; the plane defined by $\langle \rho_p, \tilde{C} \rangle = 0$ is not tangent to S and thus the existence of 'left-hand' separable states ρ_{sep} satisfying $\langle \rho_{\text{sep}}, \tilde{C} \rangle < 0$ follows. That means $\tilde{C}$ cannot be an entanglement witness (inequalities (11) are not fulfilled), see Fig. 5.

Remark. Of course, in general it is not easy to check wether the operator $\tilde{C}$ is an entanglement witness. However, for some cases (like in Sects. IV, V and VI) it is easier to apply the Lemma than using other procedures to determine the nearest separable state.

If $\tilde{C}$ is indeed an entanglement witness then, because it is tangent to S, it is optimal and can be written as $\tilde{C} = A_{opt}$, exactly like Eq. (38). It is the operator for which the GBI is maximally violated.

IV. ISOTROPIC QUBIT STATES

For illustration we present now examples. In Ref. [16] the 2-qubit Werner state has been studied – here we consider the isotropic state in 2 dimensions (acting on $\mathcal{H}^2 \otimes \mathcal{H}^2$, it is obtained for $d = 2$ in Eqs. (2), (3))

$$\rho_\alpha = \alpha \left| \phi_+^2 \right\rangle \left\langle \phi_+^2 \right| + \frac{1-\alpha}{4} \, \mathbb{1} \,, \qquad -\frac{1}{3} \le \alpha \le 1 \,, \tag{43}$$

where

$$\left| \phi_+^2 \right\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle \right) \,. \tag{44}$$

In matrix notation in the standard product basis $\{ |0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle \}$ we get

$$\rho_\alpha = \begin{pmatrix} \frac{1+\alpha}{4} & 0 & 0 & \frac{\alpha}{2} \\ 0 & \frac{1-\alpha}{4} & 0 & 0 \\ 0 & 0 & \frac{1-\alpha}{4} & 0 \\ \frac{\alpha}{2} & 0 & 0 & \frac{1+\alpha}{4} \end{pmatrix} \,, \tag{45}$$

whereas in terms of the Pauli matrices basis (17) the state can be expressed by

$$\rho_\alpha = \frac{1}{4} \left(\mathbb{1} + \alpha \, \Sigma \right) \,, \tag{46}$$

with the definition

$$\Sigma := \sigma^x \otimes \sigma^x - \sigma^y \otimes \sigma^y + \sigma^z \otimes \sigma^z \,. \tag{47}$$

We know that ρ_α is (recall Eq. (5))

$$\text{for} \quad -\frac{1}{3} \le \alpha \le \frac{1}{3} \quad \text{separable}, \qquad \text{for} \quad \frac{1}{3} < \alpha \le 1 \quad \text{entangled}\,. \tag{48}$$

To compute the Hilbert-Schmidt measure for an entangled isotropic state ρ_α^{ent} we need to calculate $D(\rho_\alpha^{\text{ent}}) = \min_{\rho \in S} \| \rho - \rho_\alpha^{\text{ent}} \|$, that is, we need to find the nearest separable state ρ_0 to the entangled state in order to obtain $D(\rho_\alpha^{\text{ent}}) = \| \rho_0 - \rho_\alpha^{\text{ent}} \|$. From the separability condition (48) we see that the state with $\alpha = 1/3$ lies on the boundary between separable and entangled isotropic states. Thus our guess for *all* isotropic entangled qubit states is (and we call it $\tilde{\rho}$):

$$\tilde{\rho} = \rho_{1/3} = \frac{1}{4} \left(\mathbb{1} + \frac{1}{3} \Sigma \right). \tag{49}$$

Now we have to check that the operator $\tilde{C}$ (42) is an entanglement witness (see Lemma in Sect. III C). For this purpose we calculate the expressions

$$\tilde{\rho} - \rho_\alpha^{\text{ent}} = \frac{1}{4} \left(\frac{1}{3} - \alpha \right) \Sigma \qquad \text{with} \quad \left\| \tilde{\rho} - \rho_\alpha^{\text{ent}} \right\| = \frac{\sqrt{3}}{2} \left(\alpha - \frac{1}{3} \right) \,, \tag{50}$$

(note that $\| \Sigma \| = 2\sqrt{3}$) and

$$\left\langle \tilde{\rho}, \tilde{\rho} - \rho_\alpha^{\text{ent}} \right\rangle = \text{Tr} \, \tilde{\rho} (\tilde{\rho} - \rho_\alpha^{\text{ent}}) = \frac{1}{4} \left(\frac{1}{3} - \alpha \right) \,. \tag{51}$$

Then the operator $\tilde{C}$ is explicitly given by

$$\tilde{C} \;=\; \frac{\tilde{\rho} - \rho_\alpha^{\mathrm{ent}} - \langle \tilde{\rho}, \tilde{\rho} - \rho_\alpha^{\mathrm{ent}} \rangle \, \mathbb{1}}{\| \tilde{\rho} - \rho_\alpha^{\mathrm{ent}} \|} \;=\; \frac{1}{2\sqrt{3}} \left(\mathbb{1} - \Sigma \right) . \tag{52}$$

We examine that $\tilde{C}$ is an entanglement witness, i.e., we check inequalities (11). For the entangled state (where $\alpha > 1/3$) we get

$$\left\langle \rho_\alpha^{\mathrm{ent}}, \tilde{C} \right\rangle \;=\; \mathrm{Tr}\, \rho_\alpha^{\mathrm{ent}} \tilde{C} \;=\; -\frac{\sqrt{3}}{2} \left(\alpha - \frac{1}{3} \right) \;<\; 0 \,. \tag{53}$$

So the first condition is satisfied. The second one, the positivity of $\langle \rho, \tilde{C} \rangle$ for all separable states ρ we see in the following way. With notation (19) for ρ_{sep} the scalar product is

$$\left\langle \rho_{\mathrm{sep}}, \tilde{C} \right\rangle \;=\; \sum_k p_k \, \frac{1}{2\sqrt{3}} \left(1 - n_x^k m_x^k + n_y^k m_y^k - n_z^k m_z^k \right) , \qquad \left| \vec{n}^k \right| \le 1, \; \left| \vec{m}^k \right| \le 1 \,. \tag{54}$$

We have to show that

$$- n_x^k m_x^k + n_y^k m_y^k - n_z^k m_z^k \;\ge\; -1 \,, \tag{55}$$

then the right-hand side of Eq. (54) remains always positive. (The convex sum of positive terms stays positive.) From the property

$$\left| \vec{n}^k \cdot \vec{m}^k \right| \;\le\; \left| \vec{n}^k \right| \left| \vec{m}^k \right| \;\le\; 1 \qquad \text{or} \qquad -1 \;\le\; \vec{n}^k \cdot \vec{m}^k \;\le\; 1 \,, \tag{56}$$

we find indeed that Eq. (55) is satisfied

$$- n_x^k m_x^k + n_y^k m_y^k - n_z^k m_z^k \;\ge\; -n_x^k m_x^k - n_y^k m_y^k - n_z^k m_z^k \;=\; -\vec{n}^k \cdot \vec{m}^k \;\ge\; -1 \,, \tag{57}$$

which completes the proof that $\langle \rho, \tilde{C} \rangle \ge 0 \; \forall \rho \in S$. So $\tilde{C}$ represents an entanglement witness

$$A_{opt} \;=\; \tilde{C} \;=\; \frac{1}{2\sqrt{3}} \left(\mathbb{1} - \Sigma \right) , \tag{58}$$

and our guess for the nearest separable state was correct, $\tilde{\rho} = \rho_0$.

The Hilbert-Schmidt measure for the entangled isotropic state is determined by Eq. (50),

$$D(\rho_\alpha^{\mathrm{ent}}) \;=\; \left\| \rho_0 - \rho_\alpha^{\mathrm{ent}} \right\| \;=\; \frac{\sqrt{3}}{2} \left(\alpha - \frac{1}{3} \right) . \tag{59}$$

It only remains to check the Bertlmann-Narnhofer-Thirring Theorem (35). Thus we calculate the maximal violation $B(\rho_\alpha^{\mathrm{ent}})$ (15) of the GBI. The maximum is attained for the optimal entanglement witness A_{opt} and the minimum for the nearest separable state ρ_0 . Then Eq. (53) determines the value of $B(\rho_\alpha^{\mathrm{ent}})$ (recall that $\langle \rho_0, A_{opt} \rangle = 0$)

$$B(\rho_\alpha^{\mathrm{ent}}) \;=\; - \left\langle \rho_\alpha^{\mathrm{ent}}, A_{opt} \right\rangle \;=\; \frac{\sqrt{3}}{2} \left(\alpha - \frac{1}{3} \right) . \tag{60}$$

So, indeed $D(\rho_\alpha^{\mathrm{ent}}) = B(\rho_\alpha^{\mathrm{ent}})$, the Hilbert-Schmidt measure equals the maximal violation of the GBI.

V.   ISOTROPIC QUTRIT STATES

Eqs. (2) and (3) define the isotropic qutrit state for $d = 3$

$$\rho_\alpha \;=\; \alpha \left| \phi_+^3 \right\rangle \left\langle \phi_+^3 \right| + \frac{1-\alpha}{9} \, \mathbb{1} \,, \qquad -\frac{1}{8} \leq \alpha \leq 1 \,, \tag{61}$$

where

$$\left| \phi_+^3 \right\rangle \;=\; \frac{1}{\sqrt{3}} \left(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle + |2\rangle \otimes |2\rangle \right). \tag{62}$$

In matrix notation in the standard product basis

$$\{ |0\rangle \otimes |0\rangle \,, |0\rangle \otimes |1\rangle \,, |0\rangle \otimes |2\rangle \,, |1\rangle \otimes |0\rangle \,, |1\rangle \otimes |1\rangle \,, |1\rangle \otimes |2\rangle \,, |2\rangle \otimes |0\rangle \,, |2\rangle \otimes |1\rangle \,, |2\rangle \otimes |2\rangle \}$$

we have

$$\rho_\alpha \;=\; \begin{pmatrix} \frac{1+2\alpha}{9} & 0 & 0 & 0 & \frac{\alpha}{3} & 0 & 0 & 0 & \frac{\alpha}{3} \\ 0 & \frac{1-\alpha}{9} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{1-\alpha}{9} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1-\alpha}{9} & 0 & 0 & 0 & 0 & 0 \\ \frac{\alpha}{3} & 0 & 0 & 0 & \frac{1+2\alpha}{9} & 0 & 0 & 0 & \frac{\alpha}{3} \\ 0 & 0 & 0 & 0 & 0 & \frac{1-\alpha}{9} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{1-\alpha}{9} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1-\alpha}{9} & 0 \\ \frac{\alpha}{3} & 0 & 0 & 0 & \frac{\alpha}{3} & 0 & 0 & 0 & \frac{1+2\alpha}{9} \end{pmatrix}. \tag{63}$$

In the Gell-Mann matrices representation (22) the state ρ_α can be expressed by (see also Ref. [27])

$$\rho_\alpha \;=\; \frac{1}{9} \left(\mathbb{1} + \frac{3\alpha}{2} \Lambda \right), \tag{64}$$

with the definition

$$\Lambda \;:=\; \lambda^1 \otimes \lambda^1 - \lambda^2 \otimes \lambda^2 + \lambda^3 \otimes \lambda^3 + \lambda^4 \otimes \lambda^4 - \lambda^5 \otimes \lambda^5 + \lambda^6 \otimes \lambda^6 - \lambda^7 \otimes \lambda^7 + \lambda^8 \otimes \lambda^8 \,. \tag{65}$$

From Eq. (5) we know that

$$\begin{aligned} -\tfrac{1}{8} \leq \alpha \leq \tfrac{1}{4} \quad &\Rightarrow \quad \rho_\alpha \;\; \text{separable} \,, \\ \tfrac{1}{4} < \alpha \leq 1 \quad &\Rightarrow \quad \rho_\alpha \;\; \text{entangled} \,. \end{aligned} \tag{66}$$

By the same argument as in the qubit case we guess the nearest separable state to the state (64)

$$\tilde{\rho} \;=\; \rho_{1/4} \;=\; \frac{1}{9} \left(\mathbb{1} + \frac{3}{8} \Lambda \right). \tag{67}$$

Again, to check our guess we examine that the operator $\tilde{C}$ (42) is an entanglement witness. We need the following expressions

$$\tilde{\rho} - \rho_\alpha^{\text{ent}} \;=\; \frac{1}{6} \left(\frac{1}{4} - \alpha \right) \Lambda \qquad \text{with} \quad \left\| \tilde{\rho} - \rho_\alpha^{\text{ent}} \right\| = \frac{2\sqrt{2}}{3} \left(\alpha - \frac{1}{4} \right), \tag{68}$$

(where $\|\Lambda\| = 4\sqrt{2}$) and

$$\left\langle \tilde{\rho}, \tilde{\rho} - \rho_\alpha^{\text{ent}} \right\rangle \;=\; \text{Tr}\, \tilde{\rho}(\tilde{\rho} - \rho_\alpha^{\text{ent}}) \;=\; \frac{2}{9}\left(\frac{1}{4} - \alpha\right). \tag{69}$$

Then $\tilde{C}$ (42) is explicitly given by

$$\tilde{C} \;=\; \frac{1}{3\sqrt{2}}\left(\mathbb{1} - \frac{3}{4}\Lambda\right). \tag{70}$$

Now let us check the entanglement witness conditions (11) for $\tilde{C}$

$$\left\langle \rho_\alpha^{\text{ent}}, \tilde{C} \right\rangle \;=\; \text{Tr}\, \rho_\alpha^{\text{ent}}\tilde{C} \;=\; -\frac{2\sqrt{2}}{3}\left(\alpha - \frac{1}{4}\right) \;<\; 0. \tag{71}$$

So the first condition is satisfied since $\alpha > 1/4$; for the second one we obtain

$$\left\langle \rho_{\text{sep}}, \tilde{C} \right\rangle \;=\; \sum_k\, p_k\, \frac{1}{3\sqrt{2}}\,(1 - n_1^k m_1^k + n_2^k m_2^k - n_3^k m_3^k - n_4^k m_4^k + n_5^k m_5^k$$
$$-\; n_6^k m_6^k + n_7^k m_7^k - n_8^k m_8^k), \qquad \left|\vec{n}^k\right| \le 1,\ \left|\vec{m}^k\right| \le 1. \tag{72}$$

Since the inequalities (56) apply here as well we have

$$-n_1^k m_1^k + n_2^k m_2^k - n_3^k m_3^k - n_4^k m_4^k + n_5^k m_5^k - n_6^k m_6^k + n_7^k m_7^k - n_8^k m_8^k \;\ge\; -\vec{n}^k \cdot \vec{m}^k \;\ge\; -1, \tag{73}$$

so that $\left\langle \rho_{\text{sep}}, \tilde{C} \right\rangle \ge 0$. Indeed, $\tilde{C}$ represents an entanglement witness and we identify

$$A_{opt} \;=\; \tilde{C} \;=\; \frac{1}{3\sqrt{2}}\left(\mathbb{1} - \frac{3}{4}\Lambda\right) \qquad \text{and} \qquad \tilde{\rho} \;=\; \rho_0. \tag{74}$$

With Eq. (68) the Hilbert-Schmidt measure is

$$D(\rho_\alpha^{\text{ent}}) \;=\; \left\|\rho_0 - \rho_\alpha^{\text{ent}}\right\| \;=\; \frac{2\sqrt{2}}{3}\left(\alpha - \frac{1}{4}\right), \tag{75}$$

and by the same argumentation as for qubits the maximal violation $B(\rho_\alpha^{\text{ent}})$ (15) of the GBI is determined by Eq. (71)

$$B(\rho_\alpha^{\text{ent}}) \;=\; -\left\langle \rho_\alpha^{\text{ent}}, A_{opt} \right\rangle \;=\; \frac{2\sqrt{2}}{3}\left(\alpha - \frac{1}{4}\right). \tag{76}$$

So again, $D(\rho_\alpha^{\text{ent}}) = B(\rho_\alpha^{\text{ent}})$, we see that the Bertlmann-Narnhofer-Thirring Theorem is satisfied.

VI. ISOTROPIC STATES IN HIGHER DIMENSIONS

Finally, we want to show how we can generalize our isotropic qubit and qutrit results to arbitrary dimensions. A general state on $\mathcal{H}^d$ can be written in a matrix basis $\left\{\mathbb{1}, \gamma^1,\ \ldots\ , \gamma^{d^2-1}\right\}$ by

$$\omega \;=\; \frac{1}{d}\left(\mathbb{1} + \sqrt{\frac{d(d-1)}{2}}\, n_i\, \gamma^i\right), \qquad \sum_i n_i^2 =: |\vec{n}|^2 \le 1. \tag{77}$$

We have included the factor $\sqrt{\frac{d(d-1)}{2}}$ for the correct normalization and the matrices γ^i have the properties

$$\operatorname{Tr}\gamma^i \ = \ 0\,, \quad \operatorname{Tr}\gamma^i\gamma^j \ = \ 2\,\delta^{ij}\,. \tag{78}$$

Considering the tensor product space $\mathcal{H}^d \otimes \mathcal{H}^d$ the notation of separable states is a straight forward extension to Eqs. (19) and (23)

$$
\begin{aligned}
\rho_{\text{sep}} \ = \ & \textstyle\sum_k \ p_k \frac{1}{d^2}\left(\mathbb{1}\otimes\mathbb{1} \ + \ \sqrt{\frac{d(d-1)}{2}}\ n_i^k\ \gamma^i\otimes\mathbb{1}\right. \\
& \left. + \ \sqrt{\frac{d(d-1)}{2}}\ m_i^k\ \mathbb{1}\otimes\gamma^i \ + \ \frac{d(d-1)}{2}\ n_i^k m_j^k\ \gamma^i\otimes\gamma^j\right)\,.
\end{aligned}
\tag{79}
$$

A $d \times d$-dimensional isotropic state – as a generalization of the isotropic qubit state (46) and qutrit state (64) – we express as

$$\rho_\alpha \ = \ \frac{1}{d^2}\left(\mathbb{1} + \frac{d}{2}\,\alpha\,\Gamma\right)\,, \qquad -\frac{1}{d^2-1}\le\alpha\le 1\,, \tag{80}$$

where we define

$$\Gamma \ := \ \sum_{i=1}^{d^2-1} c_i\,\gamma^i\otimes\gamma^i\,, \quad c_i=\pm1\,. \tag{81}$$

The factor $\frac{d}{2}$ in Eq. (80) is due to normalization. The splitting of ρ_α into entangled and separable states is given by Eq. (5).

There is strong evidence that expression (80) with definition (81) coincides with the isotropic state definition (2), (3), which we introduced in the beginning, for all dimensions $d \times d$. That means, there exist $d^2 - 1$ matrices γ^i with properties (78), which form a basis together with the identity $\mathbb{1}$ for all $d^2 \times d^2$ matrices. They describe the quantum state in the isotropic way (80), (81) and can be expressed as linear-combinations of density matrix elements in the standard basis notation.

In this way a generalization of our previous results is possible and can be obtained by calculations very similar to the ones for qubits and qutrits (see Sect. IV and Sect. V). In particular, using the same notations as before, we find the following expressions for the nearest separable state ρ_0, the Hilbert-Schmidt measure $D(\rho_\alpha^{\text{ent}})$ and the optimal entanglement witness A_{opt}:

$$\rho_0 \ = \ \rho_{\frac{1}{d+1}} \ = \ \frac{1}{d^2}\left(\mathbb{1} + \frac{d}{2(d+1)}\,\Gamma\right)\,, \tag{82}$$

$$D(\rho_\alpha^{\text{ent}}) \ = \ \left\|\rho_0 - \rho_\alpha^{\text{ent}}\right\| \ = \ \frac{\sqrt{d^2-1}}{d}\left(\alpha - \frac{1}{d+1}\right)\,, \tag{83}$$

$$A_{opt} \ = \ \frac{d-1}{d\sqrt{d^2-1}}\left(\mathbb{1} - \frac{d}{2(d-1)}\,\Gamma\right)\,. \tag{84}$$

The maximal violation of the GBI gives

$$B(\rho_\alpha^{\text{ent}}) \ = \ -\left\langle\rho_\alpha^{\text{ent}}, A_{opt}\right\rangle \ = \ \frac{\sqrt{d^2-1}}{d}\left(\alpha - \frac{1}{d+1}\right)\,, \tag{85}$$

thus we see that again $D(\rho_\alpha^{\text{ent}}) = B(\rho_\alpha^{\text{ent}})$ and Theorem (35) is satisfied.

Remark. For the limit of infinite dimensions, $d \rightarrow \infty$, the distance or the maximal violation of GBI approaches the parameter α, that means, the region where the isotropic state is separable shrinks to zero (see in this connection Refs. [33, 34]).

VII. CONCLUSIONS

In this paper we enlighten the connection between the Hilbert-Schmidt measure of entanglement and an optimal entanglement witness. This connection is viewed via the Bertlmann-Narnhofer-Thirring Theorem (35) which states that the Hilbert-Schmidt measure equals the maximal violation of a generalized Bell inequality. This inequality detects entanglement versus separability and not like the original Bell inequality non-locality versus locality. Furthermore, we present a method how to guess the nearest separable state to a given entangled state. We illustrate the general results with the examples of isotropic qubit and qutrit states and show a possible generalization of the method for isotropic states of higher dimensions.

However, we remark that in general for non-isotropic states the situation might turn out to be rather different. The reason is that our method for constructing an optimal entanglement witness, Eq. (38), involves the nearest separable state ρ_0 to a given entangled one, which in general might turn out to be a difficult task. But in some cases, like in the case of isotropic states, the Lemma presented in the article will be helpful to use.

Acknowledgments

[1] E. Schrödinger, Naturwissenschaften **23**, 807 (1935); **23**, 823 (1935); **23**, 844 (1935).

[2] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).

[3] R. A. Bertlmann and A. Zeilinger, eds., *Quantum [Un]speakables, from Bell to Quantum Information* (Springer, Berlin Heidelberg New York, 2002).

[4] Č. Brukner, M. Żukowski, and A. Zeilinger, Phys. Rev. Lett. **89**, 197901 (2002).

[5] D. Bruß, J. Math. Phys. **43**, 4237 (2002).

[6] M. Horodecki, P. Horodecki, and R. Horodecki, in *Quantum Information*, G. Alber et al., eds., *Springer Tracts in Modern Physics* 173 (Springer Verlag Berlin, 2001) p. 151.

[7] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).

[8] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).

[9] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).

[10] S. Hill and W. K. Wootters, Phys. Rev. Lett. **78**, 5022 (1997).

[11] W. K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).

[12] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight, Phys. Rev. Lett. **78**, 2275 (1997).

[13] V. Vedral and M. B. Plenio, Phys. Rev. A **57**, 1619 (1998).

[14] C. Witte and M. Trucks, Phys. Lett. A **257**, 14 (1999).

[15] M. Ozawa, Phys. Lett. A **268**, 158 (2000).

[16] R. A. Bertlmann, H. Narnhofer, and W. Thirring, Phys. Rev. A **66**, 032319 (2002).

[17] M. Horodecki and P. Horodecki, Phys. Rev. A **59**, 4206 (1999).

[18] E. M. Rains, Phys. Rev. A **60**, 179 (1999).

[19] E. M. Henley and W. Thirring, *Elementary Quantum Field Theory* (McGraw Hill, New York, 1962).

[20] B. M. Terhal, Phys. Lett. A **271**, 319 (2000).

[21] B. M. Terhal, Journal of Theoretical Computer Science **287**, 313 (2002).

[22] R. A. Bertlmann and B. C. Hiesmayr, Phys. Rev. A **63**, 062112 (2001).

[23] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).

[24] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).

[25] F. G. S. L. Brandão, Phys. Rev. A **72**, 022310 (2005).

[26] Arvind, K. S. Mallesh, and N. Mukunda, J. Phys. A: Math. Gen. **30**, 2417 (1997).

[27] C. M. Caves and G. J. Milburn, Optics Communications **179**, 439 (2000).

[28] A. O. Pittenger and M. H. Rubin, Phys. Rev. A **67**, 012327 (2003).

[29] M. Lewenstein, B. Kraus, J. I. Cirac, and P. Horodecki, Phys. Rev. A **62**, 052310 (2000).

[30] O. Guehne, P. Hyllus, D. Bruß, A. Ekert, C. Macchiavello, and A. Sanpera, J. Mod. Opt. **50**, 1079 (2003).

[31] L. M. Ioannou, B. C. Travaglione, D. Cheung, and A. Ekert, Phys. Rev. A **70**, 060303 2004.

[32] F. Verstraete, J. Dehaene, and B. D. Moor, J. Mod. Opt. **49**, 1277 (2002).

[33] K. Życzkowski, P. Horodecki, A. Sanpera, and M. Lewenstein, Phys. Rev. A **58**, 883 (1998).

[34] K. Życzkowski, Phys. Rev. A **60**, 3496 (1998).